5 leçons à retenir pour une Cybersécurité efficace

	5 leçons à retenir pour une Cybersécurité efficace

Les équipes ESET assistent régulièrement à des conférences sur la sécurité. Ils constatent que de nombreux thèmes font leur apparition : Next-gen, IoT, DDoS, plateforme d'administration des alertes complexes…

Le fait que ces mots soient de plus en plus utilisés n'est pas un problème en soi, mais nous nous sommes demandé si le monde de la cybersécurité ne prenait pas le problème dans le mauvais sens et passait alors à côté de sujets qui doivent être abordés.
À travers cette tribune, nous vous proposons 5 règles essentielles pour une sécurité efficace en entreprise.

Leçon 1 : appréhender les risques associés à l'entreprise
La sécurité informatique est complexe, mais son objectif premier est simple. Il s'agit de réduire les risques tout en les rendant visibles pour que l'entreprise puisse les accepter afin de continuer à travailler.
Pour y parvenir de manière efficace, vous devez amener vos éditeurs de solutions de sécurité à comprendre votre entreprise et à ne pas la considérer uniquement du point de vue IT, mais la saisir dans sa globalité.
En débutant un projet avec une entreprise, l'éditeur doit d'abord identifier, cartographier et catégoriser les risques y compris ceux liés spécifiquement à votre secteur d'activité (approche sectorielle). Deuxièmement, vous déterminerez ensemble les risques qui nécessitent d'être traités et dans quel ordre. Une fois cette étape réalisée, le responsable de la sécurité informatique doit mettre en place une conduite de changement avec des objectifs clairs et des délais. Idéalement, ce processus aura été pensé bien en amont et réalisé pas à pas, afin de ne pas s'engager dans trop de projets à la fois.

Leçon 2 : mettre en place une approche sécuritaire avec un but précis
La définition d'une feuille de route est essentielle et doit impliquer les responsables de l'activité de votre entreprise afin de s'adapter si cela est nécessaire. Pendant la création et l'exécution de la feuille de route, les projets définis contribueront à la réduction des risques et à l'atteinte des objectifs. Il est important de ne pas perdre de vue ces derniers pour que les responsables de la sécurité n'entravent pas la bonne marche de l'entreprise avec leurs mesures. L'approche sécuritaire définie doit être comprise par tout le monde, même sans compétences IT. Bien sûr, l'informatique joue un rôle, mais uniquement à la fin du processus lorsque les solutions sont nécessaires à l'exécution des projets de sécurité.

Leçon 3 : garantir l'essentiel avant la mise en œuvre de solutions de sécurité plus avancées
Après avoir fait le point sur les congrès auxquels nous avons assisté, nous constatons que la plupart des entreprises n'ont même pas les mesures de sécurité essentielles telles que la mise en place d'un antivirus et la protection des postes de travail par un mot de passe. Les présentations des entreprises expertes en cybersécurité offrent un contenu intéressant, mais trop avancé pour la plupart des entreprises. En outre, les retours d'expérience montrent que la grande majorité des piratages (environ 90 %) utilisent les méthodes les plus simples ou des vulnérabilités connues : courriers électroniques et phishing, pièces jointes contenant des malwares, etc. Sans oublier le maillon le plus faible : l'être humain. Vous devez donc déployer des solutions de sécurité en rapport avec ces risques connus avant de vous tourner vers des technologies de pointe plus sophistiquées, même si ces dernières sont importantes.

Leçon 4 : choisir ses fournisseurs de cybersécurité comme des partenaires
Le nombre de cybercriminels se multiplie autant que les techniques de cyberattaque (qui peuvent être très avancées). Ainsi, les solutions de sécurité ayant une protection multicouche seront indissociables de l'approche sécuritaire des entreprises. Cependant, une telle stratégie suppose comme pour toute construction de bonnes fondations. Construire un tel édifice implique une réelle coopération entre l'architecte, l'agent immobilier, le maçon, le plâtrier et bien sûr le propriétaire. Cette approche commune pour bâtir quelque chose ensemble, pas à pas, correspond exactement ce qui doit arriver dans le monde de la cybersécurité.

Leçon 5 : impliquer l'ensemble des collaborateurs pour mener à la réussite
Pour améliorer votre sécurité, vous devez avoir le soutien de vos collaborateurs. Le responsable de la sécurité doit être en mesure de fournir des explications brèves et claires à l'ensemble des métiers de la société. Si cela n'est pas réalisé correctement, votre entreprise ne comprendra pas les enjeux et ne pourra soutenir les plans définis. Comme l'a déclaré Albert EINSTEIN : « si vous ne pouvez pas expliquer quelque chose simplement, c'est que vous ne l'avez pas bien compris ! »

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cybersécurité en entreprise : 5 leçons à retenir pour une sécurité efficace – Global Security Mag Online